BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In The Matter of	)	
	)	
POLICIES AND RULES CONCERNING TOLL FRAUD	)	**CC Docket No. 93-292**
	)	

COMMENTS OF THE
TELECOMMUNICATIONS RESELLERS ASSOCIATION

The Telecommunications Resellers Association ("TRA"), by its attorneys and pursuant to Section 1.415 of the Commission's Rules, 47 C.F.R. §1.415, hereby submits its Comments in response to the Notice of Proposed Rulemaking, FCC 93-496, released December 2, 1993, in the captioned proceeding.

I.

INTRODUCTION

TRA is an association created to foster and promote the interests of entities engaged in the "switchless" resale of long distance telecommunications services both within the United States and internationally. Switchless resale involves the resale common carriage of not only the transmission capacity, but the switching capability, of underlying facilities-based carriers. Switchless resellers generally serve small and mid-sized businesses and residential customers, providing such entities and individuals with access to rates otherwise available only to much larger users. Switchless resellers also provide

their customers with a broad range of value-added services and customer support functions.

TRA's members -- more than 170 resale carriers and their underlying service and product suppliers -- range from emerging, high-growth companies to well-established, publicly-traded corporations. TRA members serve hundreds of thousands of telecommunications customers, representing more than ten billion minutes of long distance traffic annually. A relatively new market segment, the switchless resale is the fastest growing segment of the interexchange industry. Indeed, the switchless resale industry already is populated by more than 500 carriers, generates revenues in the billions of dollars and represents roughly two percent of the long distance telecommunications market.

TRA was chartered, among other things, to represent the views of its members before the Commission, other federal and state regulatory agencies and departments, legislative bodies and federal and state courts. TRA is filing comments here in furtherance of that objective. TRA also believes that it can offer the Commission a unique perspective on the issues at hand.

TRA members are both carriers and consumers of telecommunications services. As carriers, TRA members provide telecommunications services to end users or other resale carriers. TRA members, however, also purchase these same services as customers of underlying facilities-based carriers or other resale carriers. Accordingly, TRA members are liable to their underlying carriers for toll fraud perpetrated on their customers and while they may look to their customers for reimbursement, they must compensate their

underlying carriers for such fraudulent usage whether or not they collect such amounts from their customers. Further complicating this matter, TRA members control neither the network over which they provide telecommunications services to their customers nor the private branch exchanges ("PBXs") and other customer premises equipment and facilities to which they deliver those services.

TRA applauds the Commission's efforts to address the problem of toll fraud and to develop policies to allocate the liability for fraudulent use of the network among carriers, equipment manufacturers and providers, and end users. TRA submits, however, that if the Commission is to fairly and equitably allocate responsibility for toll fraud, it must take into account the unique position of TRA members as carriers without control over the networks over which their services are furnished and customers without control over the customer premises equipment to which such services are delivered. To this end, TRA urges the Commission to ensure that the tools necessary to safeguard themselves and their customers from toll fraud are made available to TRA members by underlying facilities-based carriers.

II.

ARGUMENT

A. Toll Fraud Constitutes a Very Serious Problem for Switchless Resellers.

Estimates of the extent of toll fraud losses industrywide range upward to $4, $5 and even $8 billion a year.[1] While once only the

---

[1] See, e.g., O'Shea, D., "Security Products Abound, but is Toll Fraud Too Tough," Telephony, Vol. 225, No. 9, pg. 7 (Aug. 30, 1993).

largest companies were victimized, smaller companies are increasingly being targeted as larger companies improve their security.[2] Indeed, it has been estimated that a typical PBX system now has a one in 18 chance of being "hacked" for an average loss per "hack" of $60,000.[3]

The chances that a TRA member will be victimized by toll fraud are substantially higher than those of an end-user customer. From the perspective of its underlying carrier(s), the TRA member is the customer of record for the services the TRA member provides to all of its customers. Thus, while an end user with a typical PBX system may have a one in 18 chance of being targeted by hackers, a TRA member is virtually assured of being indirectly victimized through toll fraud perpetrated on its numerous customers.

The experience of TRA members of course bears out this analysis. Virtually every TRA member has been held liable by its underlying carrier(s) for toll fraud perpetrated on its customers; indeed, most TRA members have been victimized multiple times, some for aggregate amounts ranging into the hundreds of thousands of dollars. Some TRA members look to their customers for payment of all fraudulent charges; others share the burden with customers who have been victimized. Far too often, however, smaller customers are unwilling or unable to pay the fraudulent charges, leaving TRA members to shoulder the burden alone. Because many TRA members are themselves small

---

[2] See, e.g., Communications Daily, Vol. 13, No. 187, pg. 3 (September 28, 1993).

[3] See, e.g., Steffens, C., "What You Should Know About PBX Security; Private Branch Exchange; Tracking and Stopping Hackers," Telecommunications, Vol. 27, No. 10, pg. 53 (Oct. 1993).

companies, the impact of substantial toll fraud can be extremely serious; indeed, sometimes devastating.

B. Liability For Toll Fraud Should Be Allocated To Those Best Positioned to Prevent or Minimize the Fraud.

TRA agrees with the general principal espoused by the Commission that liability for toll fraud should be allocated in accordance with relative ability to prevent or minimize such fraud. Those best positioned to control toll fraud through choice of services and use of available security and monitoring procedures and equipment should be incented to do so by imposition of some measure of liability for the fraud. Conversely, those without the ability to prevent or detect toll fraud should either be provided the tools necessary to safeguard against fraudulent network usage or be spared an allocation of toll fraud liability.

As a general matter, the entity that control and operate PBXs and other customer premises systems and equipment are in the best position to prevent fraud. Indeed, end users are the only entities that can effectively close hacker access and exit paths and install toll fraud hardware/software protection systems. For example, by eliminating remote-port access to a PBX or, on even a simpler level, by blocking calls to all or even a dozen or so international locations,[4]

---

[4] Ninety-one percent of PBX fraud losses involve calls to destinations outside the continental United States. The preponderance of these calls involve the following countries: The Dominican Republic and the 809 area code, Eqypt, Pakistan, India, the old Soviet Union, El Salvador, China, Columbia, Mexico and Ghana. O'Shea, D., "Security Products Abound, but is Toll Fraud Too Tough," Telephony, Vol. 225, No. 9, pg. 7 (Aug. 30, 1993).

an end user can virtually eliminate the threat of significant toll fraud. Use of lengthy -- i.e., eight or more digits -- access codes for direct inward system access and subjecting such multi-digit access codes to frequent change can also significantly limit exposure to toll fraud. Other security hurdles such as voice prints, human intervention, password encryption or callback can be even more effective.

By imposing restrictions on transfer capability or toll restrictions on automated attendant or voice mail equipment, an end user can block other avenues for hacker access. Hardware/software security systems that protect vulnerable points such as remote maintenance and testing ports and/or that monitor such activity as traffic levels, modem use, voice mail and direct inward system access can also be installed by the end user. And only the end user can take such basic, but nonetheless critical, steps as deleting manufacturer/vendor default passwords and deactivating trunk verification codes.

In short, the end user has available to it many effective means to prevent or at least to detect fraudulent use of its systems and equipment. The end user, accordingly, should bear the primary responsibility for safeguarding against toll fraud. An end user's failure to take reasonable steps to prevent toll fraud should be deemed to be an assumption by it of the risk of such fraud. Any other approach would eliminate the end user's incentive to take affirmative actions to prevent or minimize toll fraud.

This is not to suggest that carriers should be relieved altogether of liability for toll fraud. Because of their control of network facilities, facilities-based carriers are in a position to

minimize the impact of toll fraud on their customers. By monitoring network usage, including traffic patterns and call volumes, facilities-based carriers can detect potential fraud in real-time, provide timely notification of suspicious activity and, where warranted and authorized, take immediate action to stop fraudulent usage. Carriers are also in a position to educate customers regarding toll fraud and to assist them in safeguarding against such fraud.[5]

Switchless resellers are in a position unlike end-user customers or facilities-based carriers. They control neither customer premises equipment nor network facilities. Although they are customers, they cannot secure PBXs or ancillary facilities and although they are carriers, they cannot monitor network usage. Hence, without more, switchless resellers are not well positioned to prevent or detect toll fraud.

C. The Commission Should Require Facilities-based Carriers to Make Available to Switchless Resellers the Tools Necessary to Safeguard Themselves and Their Customers From Toll Fraud.

The Commission has tentatively concluded that carriers should bear an obligation to warn customers of the risk of toll fraud

---

[5] Equipment manufacturers and providers likewise can play an important role in the prevention of toll fraud. At a minimum, equipment manufacturers and providers can provide warnings to end users regarding the potential risks of toll fraud associated with the use of their equipment. Equipment manufacturers and providers can also play a role in educating end users regarding actions they could take to prevent or detect fraudulent usage of their facilities. And, of course, equipment manufacturers could incorporate into their equipment software and hardware functions designed to minimize toll fraud.

associated with the use of their services. Moreover, the Commission has tentatively concluded that carriers should bear a further obligation to ensure that such warnings are communicated effectively to customers through such means as billing inserts, annual notices or other information distribution methods. TRA certainly does not oppose the Commission's proposals in this respect; indeed, assisting end user efforts to prevent or minimize toll fraud redounds to the benefit of TRA members by limiting their exposure to toll fraud losses occasioned by the unwillingness or inability of their customers to pay for such fraudulent usage. TRA would welcome the opportunity to work with the Commission and other industry participants to develop appropriate educational materials and to establish effective channels of distribution for such materials.

In imposing any further obligations on carriers, however, the Commission must distinguish among those carriers that control network facilities and those that do not. A facilities-based carrier can monitor traffic patterns and volumes and temporarily suspend service in the event of suspicious activity. A switchless reseller cannot not so without the intervention of its underlying facilities-based carrier. Hence, if the Commission is to require carriers to provide monitoring services either as part of their basic service or for an additional charge, it must ensure that facilities-based carriers make these services available to their switchless-resale customers for the benefit of the switchless resellers' end-user customers.

Services such as AT&T's NetProtect, MCI Detect and SprintGUARD are not available to switchless resellers in all their permutations and hence cannot always be provided by TRA members to their customers.

Sprint, for example, states in its Tariff F.C.C. No. 2 (at Section 4.6.17(a)) that "SprintGUARD Plus is available only to Sprint's customers and will not be provided in support of the customers of any Sprint customer." AT&T's NetProtect Plus, as well as Premium and Advanced, cover only PBXs which are owned or leased by the customer of record. AT&T Tariff F.C.C. No. 1, Sections 5.7.1(A), 5.8.1(A) and 5.9.1(A). Moreover, carriers further limit coverage by requiring specified percentages of usage of their services before certain protections apply. See, e.g., id. at Section 5.7.1(A) and 5.8.1(A).

TRA urges the Commission to eliminate all direct and indirect restrictions on the availability to switchless resellers of toll fraud monitoring and detection services offered by facilities-based carriers. Certainly, the same security requirements can be imposed on a switchless reseller that are imposed on other customers. The Commission should mandate, however, that these requirements can be met indirectly by the resale carrier's end-user customers. Thus the facilities-based carrier would make available to the switchless reseller its toll fraud monitoring and detection services and the switchless reseller would be authorized to make such services available to any of its customers that satisfied the facilities-based carrier's security requirements. In short, TRA simply seeks nondiscriminatory access to services available to other customers of facilities-based carriers.

III.

CONCLUSION

By reason of the foregoing, TRA urges the Commission to adopt rules and policies in the captioned rulemaking proceeding consistent with the foregoing comments.

Respectfully submitted,

TELECOMMUNICATIONS RESELLERS ASSOCIATION

By: 

Charles C. Hunter
Kelly, Hunter, Mow & Povich, P.C.
1133 Connecticut Ave., N.W.
Seventh Floor
Washington, D.C. 20036

January 14, 1994

Its Attorneys